Amendments to the Claims

Please amend claims 1, 2, 3, 7, 8 and 9 as follows. Please add new claims 11-18. Please replace all prior versions and listings of claims in this application with the following list of claims.

---

1. (currently amended) A method for controlling access to a network ~~resources~~ resource, the method comprising:

a2

receiving at a network node, a request to assume the identity of the network node;

detecting whether the request originates with a user having a permissible virtual identity characteristic; and

if the user has a permissible virtual identity characteristic, ~~sharing~~ providing the network resource with the identity of the network node ~~with~~ in place of the identity of the user~~, wherein network resources permit access to resources by the user as if it the user had the network node identity~~.

2. (currently amended) A method for providing authorized access to a network resource, the method comprising:

receiving, at a preauthorized machine, from a first user a request to access a network resource;

detecting whether said first user is authorized to access said network resource; and

~~if said step of detecting indicates that said first user is authorized,~~

if so, assigning the first user the identity of the preauthorized machine.

3. (currently amended) The method of claim 2 further comprising:

receiving, at said preauthorized machine, from a second user a request to access a network resource detecting whether said second user is authorized to access said network resource; and

if ~~said step of detecting indicates that~~ said second user is authorized to access said network resource,

assigning the second user the identity of the preauthorized machine.

4. (original) The method of claim 3 wherein said first and second users are assigned the identity of the preauthorized machine during overlapping time periods.

5. (original) The method of claim 2 wherein said step of detecting includes,

receiving an identifier associated with the first user;

comparing the received identifier to a table of authorized identifiers; and

determining whether the received identifier matches any of the authorized identifiers based on the results of the comparing operation.

a2 cont

6. (original) The method of claim 2 wherein said step of detecting includes,

receiving a first identifier associated with the first user and a second identifier associated with a requested resource;

comparing the received first identifier/second identifier pair to contents of an authorized memory; and

determining that the user is authorized to access the requested resource if a match is found for the first and second identifier pair in the memory during the comparing step.

7. (currently amended) A method for providing access control ~~with respect to assets available on~~ to a web server, the method comprising:

providing a plurality of machines authorized to access the web server;

associating with each authorized machine an access table storing authorization information;

coupling one of the authorized machines to an access requester;

verifying that said requester is authorized to access ~~an asset~~ a resource on the web server with reference to said access table associated with the authorized machine to which the requester is coupled; and

allowing the requester to assume the identity of said authorized machine to which the ~~register~~ requester is coupled after verifying that said requester is authorized.

8. (currently amended) The method of claim 7 wherein said plurality of authorized machines includes a first authorized machine that is authorized to access a first subset of ~~assets~~ resources at the web server and a second authorized machine that is authorized to access a second subset of ~~assets~~ resources at the web server, wherein said second subset differs from said first subset.

9. (currently amended) The method of claim 7 wherein said plurality of authorized machines includes a first authorized machine that is authorized to access a first subset of ~~assets~~ resources at the web server and a second authorized machine that is authorized to access a second subset of ~~assets~~ resources at the web server, wherein said second subset overlaps with said first subset.

10. (original) The method of claim 9 wherein said first and second subsets are identical.

11. (new) A method for accessing a network resource on the Internet, comprising:

receiving at a stateful virtual identity machine within a network node, a request from a user to access the network resource;

determining if the user is authorized to access the network resource; and

if so, assigning to the user the identity of the stateful virtual identity machine, and

accessing the network resource using the assigned identity.

12. (new) The method of claim 11, wherein the network node is an Internet service provider.

13. (new) The method of claim 11, wherein the stateful virtual identity machine is pre-authorized to access the network resource.

14. (new) The method of claim 11, wherein the stateful virtual identity machine has a plurality of logical ports through which said request from the user may be received.

15. (new) A set of instructions stored in a medium to be executed by a processor to implement a method for accessing a network resource on the Internet, the method comprising:

receiving at a network node, a request from a user to access the network resource;

determining if the user is authorized to access the network resource; and

if so, accessing the network resource on behalf of the user, using the identity of the network node.

16. (new) The set of instructions of claim 15, wherein the network node is an Internet service provider.

a2 cont

17. (new) The set of instructions of claim 15, wherein the network node is pre-authorized to access the network resource.

18. (new) The set of instructions of claim 15, wherein the network node has a plurality of logical ports through which said request from the user may be received.